JUMING 聚铭
让安全更简单

聚铭安全产品

EASIER WAY FOR SECURITY

累计服务10000+政企客户

聚铭工控网络流量分析审计系统

(iCTA)

聚铭网络
www.juminfo.com

聚铭工控网络流量分析审计系统

当前，伴随工业互联网与自动控制技术的深度融合以及 5G 通信技术的普及应用，工业控制领域迎来了全新的发展机遇；同时，日趋复杂的网络环境也给工业网络安全带来了更大的挑战。各类外部攻击、病毒传播以及人为过失等工控安全事件给企业单位造成了巨大的经济损失，也导致企业单位名誉受损。

为帮助客户更好的应对工控网络安全风险，聚铭网络推出了——聚铭工控网络流量分析审计系统（iCTA）。它是一款以全流量还原为基础，结合工控网络行为审计、失陷分析、网络攻击检测、威胁情报分析、异常流量行为挖掘、文件安全检测、网络质量检测、隐蔽通道检测等技术，对工业控制系统中 IT 及 OT 网络流量全面、实时威胁感知及行为分析，是对工控安全防御系统的完善和补充，为客户在高级威胁入侵时，及时察觉、及时止损，同时也是满足国家等保、网络安全法及行业安全规范的最佳解决方案。

产品功能示意

1 行业现状

黑客大会、白帽社区的出现，导致大量工控系统软硬件设备漏洞公开，外部攻击风险逐年攀升

定向勒索、工业间谍、工业蠕虫等恶意软件层出不穷，工业系统成为勒索软件攻击青睐的目标

现状分析

1

2

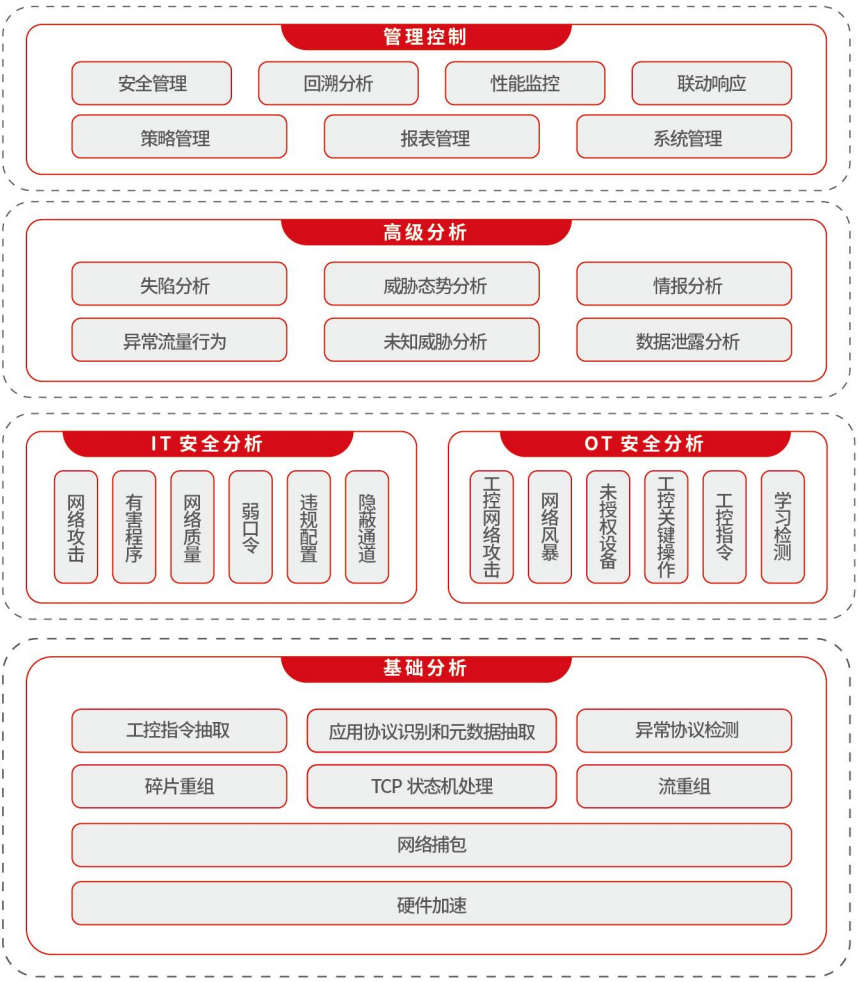
3

4

企业人为误操作、违规操作、故意破坏性操作等内部安全风险

达不到合规要求

2 系统架构



3 核心功能

工控全流量包
深度解析

工控应用
攻击检测

工控网络审计

流量异常
行为发现

网络威胁
态势感知

网络质量检测

4 产品优势

全面性网络威胁态势感知

综合外部威胁、外连威胁、内部互连威胁三个方向全面监控网络威胁态势感知情况，关注扫描探测、外部攻击、口令猜测、风险访问、C&C 回连、隐蔽通道、恶意程序活动等网络威胁行为，并支持大屏投放监控。

多维度工控网络审计

基于工控协议深度解析结果，生成工控网络会话，包括 IEC104、MODBUS、OPCDA、OPCUA、EthernetIP CIP、SINEC-H1、ENIP、MMS/S7Comm、SUPCON 等工控协议会话；支持 MODBUS、OPCUA、CIP 等工控协议指令审计，如线圈、寄存器操作等；支持对 MODBUS 关键操作审计，例如联机、上载、下载等。

1 2 3 4

多角度网络攻击检测

支持对远程代码执行、缓冲区溢出、漏洞利用等工控应用攻击检测；内置多种网络攻击检测策略，支持对一般网络攻击、明文传输、过期系统或软件、木马检测、隐蔽通道、电子加密货币活动、勒索软件、数据库攻击等进行检测。

多协议工控流量包解析

支持 IEC104、MODBUS、OPCDA、OPCUA、EthernetIP CIP、SINEC-H1、ENIP、MMS/S7Comm、SUPCON 等工控协议的精准解码、元数据提取及存储、搜索、统计。

5 技术优势

异常流量检测分析

集成聚铭网络自主研发的智能动态基线、模式信息熵等生成算法，通过一段时间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征，实施多维度的纵深检测机制，增加检测的准确性，降低误报概率。

网络质量检测分析

支持网络带宽占用异常检测、小包攻击、泛洪攻击、ARP 风暴、ICMP Flood、TCP 建连时延过长、TCP 重传过多、TCP 零窗口过多等常见的网络通讯质量问题检测，同时网络性能监控还能支持用户针对历史网络质量情况进行溯源分析。

威胁情报追踪溯源

支持恶意IP、恶意域名、恶意URL、恶意文件溯源查询，呈现威胁情报详细信息，包含情报历程、恶意标签、相关事件、相关样本等，多维数据助力威胁分析。

全流量回溯

支持针对网络协议的数据包全量留存或自定义部分留存。当发现安全事件时，可以用于上下文分析，还原“作案现场”，系统支持秒级数据包检索，并可在线分析或离线下载。

6 产品价值

NO.1

实时检测发现覆盖IT及OT的网络威胁、违规网络通讯及违规人为操作，帮助客户及时采取应对措施，规避安全风险。

NO.2

利用回溯追踪，为客户对安全事件的调查取证提供详实的数据支持。

NO.3

依托流量数据可视化，为客户呈现工控应用关键数据，提高客户工控网络运维效率。

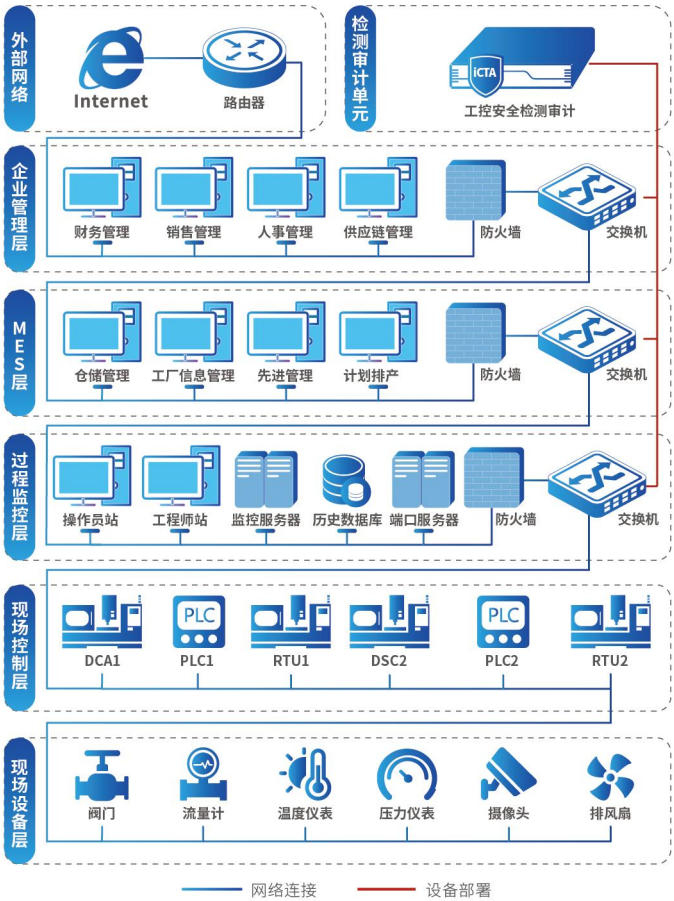
NO.4

满足如等级保护2.0、中华人民共和国工业和信息化部11号令等法律、法规对于网络数据审计的要求。

部署方式

采用旁路 SPAN 部署方式和 TAP 部署方式。

两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响。



聚铭 Juminc

聚铭订阅号

荣获国家发明专利20余项
通过【ISO9001质量管理体系认证】【ISO27001信息安全管理体系认证】
【ISO20000信息技术服务管理体系认证】
【ISO14001环境管理体系认证】【ISO45001职业健康安全管理体系认证】
【CCRC信息安全风险评估服务资质认证】【CCRC信息安全应急处理服务资质认证】

公司地址：江苏省南京市雨花台区软件大道180号南京大数据产业基地7栋4层
电话：025-52205520　　传真：025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com